



# UNITED STATES PATENT AND TRADEMARK OFFICE

48

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/000,396	11/30/2001	John A. Copeland III	10775-36246	9056

7590 05/23/2006

John R. Harris  
Morris, Manning & Martin, LLP  
1600 Atlanta Financial Center  
3343 Peachtree Rd. NE  
Atlanta, GA 30326

EXAMINER

BAUM, RONALD

ART UNIT PAPER NUMBER

2136

DATE MAILED: 05/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/000,396	COPELAND, JOHN A.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 14 March 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                                   | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>05162006</u> .  | 6) <input type="checkbox"/> Other: _____                                    |

**DETAILED ACTION**

1. This action is in reply to applicant's correspondence of 14 March 2006.
2. Claims 1- 33 are pending for examination.
3. Claims 1- 33 are rejected.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –  
(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1- 22,30,32-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Shipley, U.S. Patent 6,119,236.
5. As per claim 1; "A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious activity, comprising the steps of:  
monitoring packets exchanged between  
two hosts on the data communication network [col. 3, lines 17-col. 12, line 35,  
whereas the "... dynamically detect patterns of behavior ...", "... automatically  
determining the configuration of the LAN...", etc., clearly encompasses the claimed  
limitations, insofar as for the monitoring packets /determining /detection /comparison  
/control of the firewall to occur, that which is compared to the packet flow clearly must  
be monitored, as broadly interpreted by the examiner.];

identifying a flow corresponding to

a predetermined plurality of packets exchanged between the two hosts

that relate to a single service and

is characterized by a predetermined characteristic [col. 3, lines 17-col.

12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “...

automatically determining the configuration of the LAN...”, etc., clearly

encompasses the claimed limitations, insofar as for the monitoring packets

/determining /detection /comparison /control of the firewall to occur, that which is

compared to the packet flow clearly must be identified, and is clearly Web service

oriented (i.e., encompasses a single service which inherently ‘characterized by a

predetermined characteristic’), as broadly interpreted by the examiner.];

assigning a concern index value to an identified flow based upon

a predetermined characteristic of the flow [col. 3, lines 17-col. 12, line 35,

whereas the “... assign weight to breach...”, and “... so as a weighted average might be

used ...” aspects of the post “... look for known patterns ...”, clearly encompasses the

claimed limitations as broadly interpreted by the examiner.];

maintaining an accumulated concern index comprising

concern index values for one or more identified flows associated with a host; and

issuing an alarm signal in the event that

the accumulated concern index for a host exceeds an alarm threshold value [col.

3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react

operation ...” aspects of the post “... look for known patterns ...”, that involve the

*control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, that which is compared to the packet flow clearly must be monitored such that ‘... one or more identified flows ...’, as broadly interpreted by the examiner.].*

6. Claim 2 ***additionally recites*** the limitation that; “The method of claim 1, wherein the predetermined characteristic of a flow is selected from the group comprising:

the elapse of a predetermined period of time wherein  
no packets are exchanged between two hosts,  
the occurrence of a FIN flag,  
predetermined characteristics of traffic on a given port, and  
the occurrence of a RESET packet.”;

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, generally, and col. 6, lines 31-67 more specifically, whereas the “... access ports that do not exist ...”, and “... the multitude of responses (such as synchronization requests) forthcoming through the internet ...” aspects of “...determining a transport level protocol ...”, that involves the DOS type attack (i.e., SYN flooding use of minimal byte data field, at the transport layer whereas ‘... no packets are exchanged between two hosts ...’), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

7. Claim 3 *additionally recites* the limitation that; “The method of claim 1, further comprising the step of

communicating a message to a firewall to

drop packets going to or from the particular host in response to the alarm signal.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

8. Claim 4 *additionally recites* the limitation that; “The method of claim 1, wherein the alarm signal generates

a notification to a network administrator.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall /gateway node and subsequent “... network administrator has time to evaluate ...”, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

9. Claim 5 *additionally recites* the limitation that; “The method of claim 1,

wherein each concern index value associated with a predetermined event is

a predetermined fixed value.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... so as a weighted average might be used ...” aspects of the post “... look for known patterns ...”, clearly encompasses the claimed limitations, insofar as an average is a “predetermined fixed value”, as broadly interpreted by the examiner.).

10. As per claim 6; “A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious activity, comprising the steps of:

monitoring packets exchanged between

two hosts that are associated with

a single service on the data communications network [col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, that which is compared to the packet flow clearly must be identified, and is clearly Web service oriented (i.e., encompasses a single service which inherently ‘characterized by a predetermined characteristic’), as broadly interpreted by the examiner.];

identifying a flow corresponding to

a predetermined plurality of packets exchanged between the two hosts [col.

3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”,

*“... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, that which is compared to the packet flow clearly must be identified, and is clearly Web service oriented (i.e., encompasses a single service which inherently ‘characterized by a predetermined characteristic’), as broadly interpreted by the examiner.];*

collecting flow data from packet headers of the packets in the identified flow [col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.), as broadly interpreted by the examiner.];

based on the collected flow data, assigning a concern index value to the flow based on a predetermined characteristic of the flow [col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... so as a weighted average might be used ...” aspects of the post “... look for known patterns ...”, clearly encompasses the claimed limitations, as broadly interpreted by the examiner.];

maintaining an accumulated concern index from flows that are

associated with a particular host;

issuing an alarm signal in the event that

the accumulated concern index for the particular host exceeds



an alarm threshold value [col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and  
in response to the alarm signal,

sending a message to a utilization component [col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations, insofar as network associated firewall /gateway node notification is clearly signaling a utilization component, as broadly interpreted by the examiner.].

11. Claim 7 **additionally recites** the limitation that; “The method of claim 6, wherein the utilization component is selected from the group comprising:

network security device,  
email,  
SNMP trap message,  
beeper,  
cellphone,  
firewall,  
network monitor,

user interface display to an operator.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall /gateway node and subsequent “... network administrator has time to evaluate ...”, clearly encompasses the claimed limitations, insofar as a network associated firewall /gateway node is a network security device, firewall, and network monitor utilization component, as broadly interpreted by the examiner.).

12. As per claim 8; “A method of analyzing network communication traffic on a data communication network for determining whether the traffic is legitimate or potential suspicious activity, comprising the steps of:

monitoring the exchange of packets between

two hosts each having a particular Internet Protocol (IP) address [col. 3, lines 17-col. 12, line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

identifying a flow corresponding to

a predetermined plurality of packets exchanged between

a particular port of one of the hosts that

remains constant during the plurality of packets [col. 3, lines 17-  
col. 12, line 35, whereas the “... dynamically detect patterns of behavior  
...”, “... automatically determining the configuration of the LAN...”, etc.,  
clearly encompasses the claimed limitations, insofar as for the monitoring  
packets /determining /detection /comparison /control of the firewall to  
occur, that which is compared to the packet flow clearly must be  
identified, and is clearly Web service oriented (i.e., encompasses a single  
client/server service which inherently ‘remains constant’ throughout the  
servicing of said service request/response), as broadly interpreted by the  
examiner.];

collecting flow data from

packet headers of the packets in the identified flow [col. 3, lines 17-col. 12, line 35,  
whereas the “... dynamically detect patterns of behavior ...”, “... automatically  
determining the configuration of the LAN...”, etc., clearly encompasses the claimed  
limitations, insofar as for the determining /detection /comparison /control of the firewall  
to occur, the packet flow clearly must be collected per se, and such collection involves  
collection of the packets header data (i.e., the IP address, port, status flags, etc.), as  
broadly interpreted by the examiner.];

based on the collected flow data,

assigning a concern index value to the flow [col. 3, lines 17-col. 12, line 35,  
whereas the “... assign weight to breach...”, and “... so as a weighted average might be

*used ...” aspects of the post “... look for known patterns ...”, clearly encompasses the claimed limitations, as broadly interpreted by the examiner.];*

maintaining a host data structure containing

accumulated concern index values from

a plurality of flows that are associated with the particular host; and

issuing an alarm in the event that

the accumulated concern index values for the particular host has

*exceeded an alarm threshold value [col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations as broadly interpreted by the examiner.].*

13. Claim 9 ***additionally recites*** the limitation that; “The method of claim 8, wherein each concern index value associated with a respective potential suspicious activity is a predetermined fixed value.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... so as a weighted average might be used ...” aspects of the post “... look for known patterns ...”, clearly encompasses the claimed limitations, insofar as an average is a “predetermined fixed value”, as broadly interpreted by the examiner.).

14. As per claim 10, this claim is the apparatus/system for the method claim 6 above, and is

rejected for the same reasons provided for the claim 6 rejection; “A system for analyzing network communication traffic and determining potential suspicious activity, comprising:

a computer system operative to:

- a) monitor the communication of packets on a data communication network;
  - b) classify the monitored packets into flows, wherein a flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;
  - c) analyze the flows in order to assign a concern index value to a flow that may signify potential suspicious activity, wherein each concern index value associated with a respective potential suspicious activity is of a predetermined fixed value;
  - d) generate an alarm signal in response to cumulated concern index values;
- and

a communication system coupled to the computer system operative to receive packets communicated between hosts on the network.”

15. As per claim 11, this claim is the apparatus/system for the node processor element with associated database element for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; “A system for analyzing network communication traffic and determining potential suspicious activity, comprising:

a processor operative to:

- a) monitor the communication of packets on a data communication network;
- b) classify the monitored packets into flows, wherein a flow corresponds to a predetermined plurality of packets exchanged between two hosts that are associated with a single service on the network;
- c) maintain a flow data structure for storing data corresponding to a plurality of flows;
- d) analyze the flows in the flow data structure in order to assign a concern index value to a flow that may signify potential suspicious activity, wherein each concern index value associated with a respective potential suspicious activity is of a predetermined fixed value;
- e) cumulate assigned concern index values of one or more flows associated with a particular host;
- f) maintain a host data structure for storing data associating a cumulated concern index value with each one of a plurality of hosts; and
- g) generate an alarm signal in response to cumulated concern index values in the host data structure;

a memory coupled to the processor and operative to store the flow data structure and the host data structure; and

a network interface coupled to the processor operative to receive packets on the data communication network.”

16. As per claim 12, this claim is a specific attack method for claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; “A method of analyzing network communication traffic on a data communication network for potential suspicious activity, comprising the steps of:

monitoring packets exchanged between

two hosts on the data communication network;

identifying packets provided by one of the two hosts that have

a transport level protocol specifying a packet format that includes a data segment;

in response to determination that

the transport level protocol is a User Datagram Protocol (UDP) packet and

the data segment associated with the UDP packet contains two bytes or less of

data,

storing a concern index value of a predetermined amount in

a memory in association with information identifying the host that issued the UDP packet [col. 3, lines 17-col. 12, line 35, generally, and col. 6, lines 31-67 more specifically, whereas the “... access ports that do not exist ...”, and “... the multitude of responses (such as synchronization requests) forthcoming through the internet ...” aspects of “...determining a transport level protocol ...”, that involves the DOS type attack (i.e., SYN flooding use of minimal byte data field, at

*the transport layer), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and*

issuing an alarm when

the cumulated concern index value associated with the host exceeds a predetermined threshold level.”

17. Claim 13 *additionally recites* the limitation that; “The method of claim 6, wherein a flow is characterized by a predetermined characteristic selected from the group comprising:

the elapse of predetermined period of time where

no packets are exchanged between two hosts,

the occurrence of a FIN flag,

predetermined characteristics of traffic on a given port, and

the occurrence of a RESET packet.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, generally, and col. 6, lines 31-67 more specifically, whereas the “... access ports that do not exist ...”, and “... the multitude of responses (such as synchronization requests) forthcoming through the internet ...” aspects of “...determining a transport level protocol ...”, that involves the DOS type attack (i.e., SYN flooding use of minimal byte data field, at the transport layer whereas ‘... no packets are exchanged between two hosts ...’), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).



18. Claim 14 *additionally recites* the limitation that; “The method of claim 8, wherein a flow is characterized by a predetermined characteristic selected from the group comprising:

the elapse of predetermined period of time where  
no packets are exchanged between two hosts,  
the occurrence of a FIN flag,  
predetermined characteristics of traffic on a given port, and  
the occurrence of a RESET packet.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, generally, and col. 6, lines 31-67 more specifically, whereas the “... access ports that do not exist ...”, and “... the multitude of responses (such as synchronization requests) forthcoming through the internet ...” aspects of “...determining a transport level protocol ...”, that involves the DOS type attack (i.e., SYN flooding use of minimal byte data field, at the transport layer whereas ‘... no packets are exchanged between two hosts ...’), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

19. Claim 15 *additionally recites* the limitation that; “The method of claim 10, wherein a flow is characterized by a predetermined characteristic selected from the group comprising:

the elapse of predetermined period of time where  
no packets are exchanged between two hosts,  
the occurrence of a FIN flag,  
predetermined characteristics of traffic on a given port, and  
the occurrence of a RESET packet.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, generally, and col. 6, lines 31-67 more specifically, whereas the "... access ports that do not exist ...", and "... the multitude of responses (such as synchronization requests) forthcoming through the internet ..." aspects of "...determining a transport level protocol ...", that involves the DOS type attack (i.e., SYN flooding use of minimal byte data field, at the transport layer whereas '... no packets are exchanged between two hosts ...'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

20. Claim 16 *additionally recites* the limitation that; "The method of claim 11, wherein a flow is characterized by a predetermined characteristic selected from the group comprising:

the elapse of predetermined period of time where

no packets are exchanged between two hosts,

the occurrence of a FIN flag,

predetermined characteristics of traffic on a given port, and

the occurrence of a RESET packet."

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, generally, and col. 6, lines 31-67 more specifically, whereas the "... access ports that do not exist ...", and "... the multitude of responses (such as synchronization requests) forthcoming through the internet ..." aspects of "...determining a transport level protocol ...", that involves the DOS type attack (i.e., SYN flooding use of minimal byte data field, at the transport layer whereas '... no packets are exchanged between two hosts ...'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

21. Claim 17 *additionally recites* the limitation that; “The method of claim 1, wherein the single service comprises

a port number remaining constant for a plurality of packets.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, that which is compared to the packet flow clearly must be identified, and is clearly Web service oriented (i.e., encompasses a single client/server service which inherently ‘remains constant’ throughout the servicing of said service request/response), as broadly interpreted by the examiner.).

22. Claim 18 *additionally recites* the limitation that; “The method of claim 1, wherein the suspicious activity is

from an inside address or

from an outside address.”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, that which is compared to the packet flow clearly must be identified, and is clearly Web service

oriented (i.e., encompassing intranet (inside address) and internet (outside address) aspects of the Internet), as broadly interpreted by the examiner.).

23. Claim 19 *additionally recites* the limitation that; “The method of claim 1, wherein the concern index for a suspicious activity is

derived by reference to a table of predetermined suspicious activities each having  
a predetermined concern index value. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as it is inherent that data structure referencing in computers (i.e., exception handling, OSI stack processing, object referencing, and associated operating system functionality) encompasses table/indexed referencing of said data structures, as broadly interpreted by the examiner.).

24. Claim 20 *additionally recites* the limitation that; “The method of claim 1, wherein the host for which the concern index is

accumulated is an inside host. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, that

which is compared to the packet flow clearly must be identified, and is clearly Web service oriented (i.e., encompassing intranet (inside address) and internet (outside address) aspects of the Internet), as broadly interpreted by the examiner.).

25. Claim 21 *additionally recites* the limitation that; “The method of claim 1, wherein the host for which the concern index is  
accumulated is an outside host. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, that which is compared to the packet flow clearly must be identified, and is clearly Web service oriented (i.e., encompassing intranet (inside address) and internet (outside address) aspects of the Internet), as broadly interpreted by the examiner.).

26. Claim 22 *additionally recites* the limitation that; “The method of claim 1, wherein the steps are carried out in  
a monitoring appliance. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the

monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a 'monitoring appliance', as broadly interpreted by the examiner.).

27. Claim 30 ***additionally recites*** the limitation that; "The method of claim 1, wherein the monitoring of packets comprises

monitoring on packet header information only. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the "... dynamically detect patterns of behavior ...", "... automatically determining the configuration of the LAN...", etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.), as broadly interpreted by the examiner.).

28. Claim 32 ***additionally recites*** the limitation that; "The method of claim 1, wherein the alarm signal is provided to

a utilization component. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations, insofar as network associated firewall /gateway node notification is clearly signaling a utilization component, as broadly interpreted by the examiner.).

29. Claim 33 **additionally recites** the limitation that; “The method of claim 32, wherein the utilization component is selected from the group comprising:

network security device,

email,

SNMP trap message,

beeper,

cellphone,

firewall,

network monitor,

user interface display to an operator. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... assign weight to breach...”, and “... react operation ...” aspects of the post “... look for known patterns ...”, that involve the control and notification of the network associated firewall /gateway node, clearly encompasses the claimed limitations, insofar as network associated firewall /gateway node notification is clearly signaling a utilization component, as broadly interpreted by the examiner.).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

Art Unit: 2136

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

30. Claims 23-29,31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shipley, U.S. Patent 6,119,236 and further in view of below.

It is noted that Shipley does not disclose in the base software the specific associated standard LAN to Internet network components per se (i.e., routers relative to firewall(s)/gateways/inline filter(s) relative to LAN inside/outside/DMZ routing components). However, the examiner asserts that it would have been obvious to one ordinary skill in the art at the time the invention was made to configure the network components generally, and the Shipley device more particularly, in the various network components so configured as per the dependent claim limitations below. A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)).

31. Claim 23 *additionally recites* the limitation that; "The method of claim 22, wherein the monitoring appliance is installed  
behind a firewall."

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the "... dynamically detect patterns of behavior ...", "... automatically determining the configuration of the LAN...", etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a 'monitoring appliance' whereas it would be obvious to one ordinary skill in



the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

32. Claim 24 *additionally recites* the limitation that; “The method of claim 22, wherein the monitoring appliance is connected

before a firewall. ”.

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a ‘monitoring appliance’ whereas it would be obvious to one ordinary skill in the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

33. Claim 25 *additionally recites* the limitation that; “The method of claim 22, wherein the monitoring appliance is connected

in a DMZ. ”.

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a ‘monitoring appliance’ whereas it would be obvious to one ordinary skill in

Art Unit: 2136

the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

34. Claim 26 *additionally recites* the limitation that; “The method of claim 22, wherein the monitoring appliance is configured to

operate as a pass-by filter. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a ‘monitoring appliance’ whereas it would be obvious to one ordinary skill in the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

35. Claim 27 *additionally recites* the limitation that; “The method of claim 22, wherein the monitoring appliance is coupled to

a network device. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a ‘monitoring appliance’ whereas it would be obvious to one ordinary skill in

the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

36. Claim 28 *additionally recites* the limitation that; “The method of claim 27, wherein the network device is selected from group comprising:

router,

switch,

hub,

tap. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a ‘monitoring appliance’ whereas it would be obvious to one ordinary skill in the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

37. Claim 29 *additionally recites* the limitation that; “The method of claim 27, wherein the network device is

a network security device. ”.

The teachings of Shipley suggest such limitations (col. 3, lines 17-col. 12, line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the

configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a ‘monitoring appliance’ whereas it would be obvious to one ordinary skill in the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

38. Claim 31 *additionally recites* the limitation that; “The method of claim 1, wherein the monitoring of packets is

carried out in a device operating in a promiscuous mode. ”.

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the “... dynamically detect patterns of behavior ...”, “... automatically determining the configuration of the LAN...”, etc., clearly encompasses the claimed limitations, insofar as for the monitoring packets /determining /detection /comparison /control of the firewall to occur, said firewall constitutes a ‘monitoring appliance’ whereas it would be obvious to one ordinary skill in the art at the time the invention was made to configure the network for intended use, as broadly interpreted by the examiner.).

### ***Response to Amendment***

39. As per applicant’s argument concerning the lack of teaching by Shipley of the packet flow based aspects of the invention, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive in light of the still broad and nebulous nature of the phrase ‘flow ...’ as associated with the Shipley ‘patterns of activity ...’

aspects of the rejection. Therefore, at a granularity level that would encompass delineation by header, payload and trailer, the various Shipley reference data stream header/payload/field protocol delineations, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that the rejection support reference collectively encompass the said claim limitations in their entirety.

40. As per applicant's argument concerning the lack of teaching by Shipley of the packet flow based aspects of the invention, as related to packet headers per se, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive in light of the still broad and nebulous nature of the phrase 'flow ...' as discussed above, and further in respect to the rejection comments as discussed in the particular claims rejections.

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

*Conclusion*

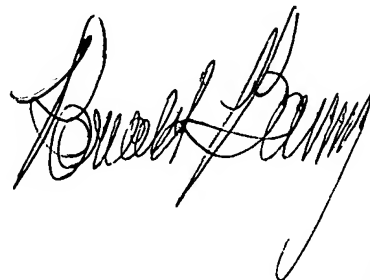
41. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner



AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100